BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
New Part 4 of the Commission's Rules	)	ET Docket No. 04-35
Concerning Disruptions to Communications	)	

TO: The Commission

COMMENTS OF THE DEPARTMENT OF HOMELAND SECURITY

By: Joe D. Whitley
General Counsel
UNITED STATES DEPARTMENT OF HOMELAND SECURITY
700 D Street, S.W.
Washington, D.C. 20528
(202) 692-4232

Thomas J. Connelly
Associate General Counsel for
Information Analysis and Infrastructure Protection
UNITED STATES DEPARTMENT OF HOMELAND SECURITY
Nebraska Avenue Complex
Washington, D.C. 20528
(202) 282-8395

Eric T. Werner
UNITED STATES DEPARTMENT OF HOMELAND SECURITY
Office of the General Counsel
700 D Street, S.W.
Washington, D.C. 20528
(202) 401-0775

Its Attorneys

Date: June 2, 2004

TABLE OF CONTENTS

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
New Part 4 of the Commission's Rules	)	ET Docket No. 04-35
Concerning Disruptions to Communications	)	

TO: The Commission

COMMENTS OF THE DEPARTMENT OF HOMELAND SECURITY

The UNITED STATES DEPARTMENT OF HOMELAND SECURITY (DHS), by its attorneys, and pursuant to Section 1.415 of the rules of the Federal Communications Commission ("FCC" or "Commission"), 47 C.F.R. § 1.415 (2003), hereby submits these Comments jointly on behalf of its Directorate for Information Analysis and Infrastructure Protection ("IAIP") and the National Communications System ("NCS")[1] in response to the Commission's Notice of Proposed Rule Making in the proceeding captioned above ("Notice").[2]

I. INTRODUCTION AND SUMMARY

As the Commission's Notice observes, the modern telecommunications system upon which our nation relies no longer consists solely, or even primarily, of wireline-based facilities, but encompasses a network of interconnected technological platforms including terrestrial wireless, satellite, and cable.[3] DHS agrees with the Commission that the same need to ensure the

---

[1] Executive Order No. 12472 of April 3, 1984, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, 49 Fed. Reg. 13471 (1984), established the National Communications System. Executive Order No. 13286 of February 26, 2003, § 46(b), 68 Fed. Reg. 10619, 10627, designated the Secretary of Homeland Security as Executive Agent of the NCS, and it is in that capacity that he submits these comments its on behalf.

[2] *New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, FCC 04-30, released February 23, 2004 (Notice of Proposed Rule Making in ET Docket No. 04-35), summary published at 69 Fed. Reg. 15761 (March 26, 2004) [hereinafter "*Notice*"]. Unless otherwise noted, citations to the *Notice* will be to the FCC document, FCC 04-30. The deadline for filing comments in this proceeding was May 25, 2004. Accordingly, DHS is filing concurrently with these comments, under separate cover, a *Motion to Accept Late-Filed Comments*.

[3] *See Notice* at 5 ¶ 5 and accompanying notes.

robustness and reliability of the nation's telecommunications that supported the collection of outage information for wireline providers over a decade ago now makes collecting specific outage data for these other technological platforms equally important.

Such service disruption information is critical to NCS' ability to plan for, mitigate, respond to, and recover from events that threaten national security/emergency preparedness ("NS/EP") telecommunications, as well its capacity to ensure the availability of Priority Services as directed by the President. The availability of such information also enhances the effectiveness of IAIP's efforts to secure the nation's critical infrastructure as a whole. In each of these ways, collection of the information contributes significantly to protecting our homeland and preserving our national and economic security.

DHS appreciates the Commission's effort in the Notice to balance the needs of all stakeholders to maintain and expand the Federal government's collaborative partnership with all industry participants. This partnership provides an important foundation for coordinating government and private sector efforts to ensure reliable telecommunications for the nation. In the spirit of this partnership, DHS would not object to adoption of a voluntary reporting framework; however, in light of the history of past voluntary reporting trials, DHS could support such an approach only if clear evidence exists of a firm commitment from all service providers to participate fully in the program.

Regardless of whether a voluntary or mandatory approach is adopted, however, DHS urges the Commission to direct that the outage reports be filed with the National Coordinating Center for Telecommunications-Information Sharing and Analysis Center ("NCC Telecom-ISAC"). As discussed herein, such an arrangement is appropriate in light of the leadership and operational responsibilities that the President and Congress have charged IAIP/NCS to perform. It is also sensible from a policy standpoint because the NCC Telecom-ISAC is ideally equipped

both to (1) put the outage information to immediate use in connection with any response or restoration activities that the outage in question may require; and (2) expeditiously channel the information into the ISAC's analytical and collaborative processes for the purposes of identifying, developing, validating, and sharing new best practices and testing and refining existing ones.

Most importantly, DHS strongly believes that the Commission should change its existing policy of making outage reporting data generally available and easily accessible to the public. Whatever merit this approach may have had when the outage reporting rules were first adopted, the threat environment following September 11, 2001, dictates that appropriate steps be taken, consistent with law, to safeguard sensitive information, like that included in the outage reports, which could jeopardize our security efforts if disclosed to inappropriate recipients.

The same outage data that can be so useful for the purpose to identify and remedy critical vulnerabilities and make the network infrastructure stronger can, in hostile hands, be used to exploit those vulnerabilities to undermine or attack networks. Moreover, ready public access to outage reports is not necessary to the development of best practices. Several public-private bodies (*e.g.*, NCC Telecom-ISAC and the Network Security Information Exchange ("NSIE")) now exist that support information sharing in a safe environment and foster collaboration within industry to develop effective best practices.

Finally, while it supports the Commission's proposal to adopt a user-based standard to gauge whether a particular disruption or outage is significant enough to warrant reporting, DHS questions whether the proposed "common metric" of 30-minute/900,000-user minutes is either suitable or appropriate to apply on a uniform basis across all segments. DHS will await the comments from industry concerning these important technical issues and urges the Commission to reexamine its proposed standard carefully in light of that input.

DHS is coordinating closely with its partners and looks forward to working closely with industry and the Commission to achieve a reporting framework that delivers the information essential to maintaining the integrity and resilience of America's critical telecommunications infrastructure for NS/EP and homeland security purposes while also appropriately safeguarding the information and addressing carriers' concerns about the potential costs and burdens of the program.

II. STATEMENT OF INTEREST AND POSITION

The Commission is well acquainted with NCS; the two agencies have worked together on many important issues of common concern.[4] Established by Executive Order No. 12472, of April 3, 1984, the NCS is an interagency organization that combines the communications assets of 23 Federal departments and agencies to address NS/EP telecommunications related issues. NCS provides guidance and assistance on NS/EP telecommunications issues to the President, the National Security Council ("NSC"), the Homeland Security Council, the Director of the Office of Science and Technology Policy ("OSTP"), and the Director of the Office of Management and Budget ("OMB") concerning a range of national security matters including the coordination of, planning for, and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.[5]

As part of the realignment of Federal government responsibilities following the events of September 11, 2001, the President designated the Secretary of Homeland Security as the Executive Agent for NCS.[6] In addition, the Office of the Manager, NCS ("OMNCS") was

---

4 *See*, *e.g.*, *id.* at 10 ¶ 14 n.39.

5 *See* E.O. No. 12472 § 1(b), as amended by E.O. No. 13286 of February 26, 2003.

6 E.O. No. 13286 § 46(b), 68 Fed. Reg. 10619, 10627.

transferred from the Defense Information Systems Agency into IAIP.[7] As part of the Office of Infrastructure Protection ("IP") of IAIP, OMNCS (acting on behalf of the NCS Committee of Principals and the Executive Agent) oversees efforts to carry forward NCS' mission to ensure that the telecommunications infrastructure of the United States:

- meets the NS/EP needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of government;
- Can satisfy priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources;
- Incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to maintain the survivability of NS/EP telecommunications in all circumstances, and
- Comports, to the maximum extent practicable, with other national telecommunications policies.[8]

Working collectively with its counterpart divisions within IP – the Infrastructure Coordination Division ("ICD"), the National Cyber Security Division ("NCSD"), and the Protective Security Division ("PSD") – OMNCS integrates telecommunications assurance efforts with IAIP's overall strategy for critical infrastructure protection across all of the critical sectors.

In addition to its duties under the Homeland Security Act,[9] IAIP also holds operational responsibility for the Secretary's responsibilities under Homeland Security Presidential Directive 7 ("HSPD-7"), including "coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States" generally and, more specifically, to "coordinate protection activities for . . . critical infrastructure sectors . . . [including] information technology; [and] telecommunications . . . ."[10]

---

7 Homeland Security Act of 2002 § 201(g)(2) ["Act"], codified at 6 U.S.C. § 121(g)(2).

8 E.O. No. 12472 § 1(c), as amended by E.O. No. 13286 of February 26, 2003.

9 *See* Act § 201(d), 6 U.S.C. 121(d).

10 Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and*

The Commission makes clear in the Notice that it is these very homeland security concerns, for which DHS/IAIP and specifically NCS have primary responsibility within the Federal government, that motivated the commencement of this proceeding and that underlie the proposed rules.[11] Accordingly, IAIP and NCS have acute interests in the rules ultimately adopted by the Commission in this proceeding.[12]

III. REPORTING OF NON-WIRELINE SERVICE DISRUPTION INFORMATION WILL PROMOTE NS/EP TELECOMMUNICATIONS AND SIGNIFICANTLY ENHANCE CRITICAL INFRASTRUCTURE PROTECTION EFFORTS

At the outset of the Notice, the Commission requests comment on its conclusion that "service disruption reporting by non-wireline communications providers will provide benefits similar to those" realized from such reports provided by wireline communications providers.[13] DHS supports the need for communications disruption reporting that includes all platforms and concurs with the Commission's conclusion.

As the Notice sets forth in detail, terrestrial wireless, cable, and satellite services have expanded exponentially in the last decade and have become important alternatives to traditional wireline telephony for transmitting voice and data, and they have taken on increasing

(..continued)
Protection, December 17, 2003 ¶¶ 12, 15. HSPD-7 also assigns to the Secretary leadership responsibility for the nation's cyber security efforts, charging him to maintain an organization (the NCSD) to serve as the "focal point" for cyberspace security that has as its mission: "analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems." *Id.* ¶ 16. Thus, to the extent that the nation's telecommunications infrastructure provides the backbone for a significant amount of Internet traffic, DHS has a direct interest in telecommunications service disruption information.

[11] *Notice* at 3-5 ¶¶ 3-5. Notably, although the Notice treats them as somehow distinct from homeland security interests, even the sections of the Communications Act quoted by the Commission articulate purposes and objectives that fall squarely in the zone of homeland security, namely, ". . . *the purpose of the national defense [and] for the purpose of promoting safety of life and property*." *See id*. at 4 ¶ 4, quoting 47 U.S.C. § 151 (emphasis in original).

[12] Moreover, DHS, through the United States Coast Guard (USCG), also has responsibility for maritime safety and security in the United States. Because of the growing reliance that recreational boaters and commercial marine operators place on wireless and satellite communications for a wide array of navigational and maritime safety purposes, the Commission's proposed rules concerning reporting of disruptions of these services also are of acute importance to the USCG.

[13] *Notice* at 5 ¶ 4.

significance for homeland security, emergency response, and national security functions.[14] This convergence of technology makes collection of service disruption information from these other platforms critical for IAIP/NCS planning for homeland security and NS/EP communications.[15]

Data concerning such subjects as the precipitating cause(s), surrounding circumstances, scope and gravity of impacts, and the effectiveness or not of actions taken to respond to a network outage or disruption are prerequisite to the analysis that supports efforts to abate or reduce system vulnerabilities. They can reveal, for example, whether service outages or disruptions stem from anomalous events or circumstances or are systemically based and can, thus, provide insight into appropriate remedial or protective measures.

Reporting of non-wireline service disruption information will also promote improved maritime distress and safety communications with the Coast Guard. A growing number of recreational boaters and commercial mariners increasingly depend on wireless and mobile satellite communications for reporting and receipt of navigational and meteorological safety information, medical emergencies, distress alerting to the USCG and other safety communications. Timely notification of outages in these services could allow the Coast Guard to take measures to minimize the disruption of maritime safety.

DHS concurs with the Commission's assessment that the availability of outage data from wireline providers has contributed to the development and refinement of voluntary industry best practices. The voluntary evolution of best practices through such bodies as the Network Reliability and Interoperability Council ("NRIC") and the Network Reliability Steering

---

[14] *Id.* at 9-11 ¶¶ 14-17.

[15] Although the Notice observes that public data networks utilizing the Internet have also played an important role in emergency response and homeland defense efforts, the Commission states that it is "not proposing, at this time, to adopt reporting requirements for public data networks." *Id.* at 4-5 ¶ 4 and n.4. DHS believes that, as the volume of traffic carried on a voice over Internet protocol (VoIP) basis continues to expand, the Internet will commensurately become a more important part of the telecommunications infrastructure. For this reason, DHS urges the Commission to revisit the topic of Internet outage reporting in the future as the nature, criteria, and most

Committee ("NRSC") has, in turn, led to vast improvements in system reliability. Adding information concerning non-wireline communications service disruptions to that already being furnished by wireline service providers will enhance IAIP/NCS' capacity, as well as that of other government bodies (*e.g.*, the Commission and State public utility commissions), and the carriers themselves, to analyze vulnerabilities and develop mitigation strategies and plan appropriate response and restoration measures, yielding additional significant dividends for homeland and national security.

DHS specifically recommends that the Commission explore methods to make outage information available to the State public utilities commissions (PUCs). Such information sharing would reduce the need for States regulators to collect intrastate outage data independently. This would address a key concern expressed by carriers relative to the costs and administrative burdens associated with potentially redundant reporting schemes across levels of government and among multiple States. Moreover, because much of the reported data would likely constitute "homeland security information" under Federal law,[16] sharing the information with State authorities through such channels would also facilitate more effective safeguarding of this sensitive information against disclosure to those who might desire to use it for hostile purposes.[17] This issue is discussed in greater depth in Section VI, *infra.*

(..continued)
appropriate mechanisms for addressing the IP-based infrastructure become clearer.

[16] *See* Homeland Security Act § 892(f)(1) [hereinafter "Act"], codified at 6 U.S.C. § 482(f)(1). "Homeland security information" consists, in relevant part, of "any information possessed by a Federal, State, or local agency that — . . . (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; . . . or (D) would improve the response to a terrorist act." *Id.*

[17] Pursuant to Section 892 of the Act, 6 U.S.C. § 482, and Executive Order No. 13311 of July 29, 2003, 68 Fed. Reg. 45149, DHS is presently developing procedures to facilitate the handling and sharing of homeland security information among the departments and agencies of Federal government and between the Federal government and State and local governments and certain members of the private sector that affect critical infrastructure, cyber, economic, or public health security. Section 892(e) of the Act prescribes that

> information obtained by a State or local government from a federal agency" under these procedures, "shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to

IV. DHS WOULD SUPPORT VOLUNTARY REPORTING UPON SATISFACTORY EVIDENCE THAT ALL SERVICE PROVIDERS ARE COMMITTED TO PARTICIPATE FULLY. IN ANY EVENT, THE FCC SHOULD DESIGNATE THE NCS' NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS-INFORMATION SHARING AND ANALYSIS CENTER (NCC TELECOM-ISAC) AS THE PRIMARY RECIPIENT OF OUTAGE DATA

A. *Mandatory versus Voluntary Reporting*

Noting the success of efforts to identify, validate, and improve industry best practices that has been achieved under the existing reporting framework, the Notice observes that "[t]his process would likely not have been possible or so successful if service disruption reporting had not been mandatory and if those reports had not been available to communications providers, manufacturers, and the public."[18] Notwithstanding this view, however, the Commission invites comment on whether a voluntary program of outage reporting could be structured to assure that all carriers file accurate and complete reports on a reliable basis, including during significant disruption events or transitions in company management.[19]

DHS stresses the essential nature of the timely receipt of outage reporting data from all industry members in support of planning and response. DHS understands the Commission's view that mandatory reporting of the data may be necessary for industry coordination efforts to succeed. However, while DHS is aware of the uneven results that voluntary reporting trial programs have yielded in the past,[20] industry is working to improve its reporting systems and increase participation. Therefore, in light of this information and the Commission's request for comments, DHS is not opposed to a voluntary reporting structure,[21] provided there is persuasive

(..continued)
such information.

6 U.S.C. § 482(e).

[18] *Notice* at 8 ¶ 10.

[19] *Id.* ¶ 12.

[20] *See Notice* at 8 ¶ 11 & n.28.

[21] For example, DHS believes that such bodies as NCC Telecom-ISAC and the Network Security Information Exchange (NSIE) provide highly effective mechanisms for members of industry to share information jointly, with

evidence of an absolute commitment from all carriers in the relevant industry segments to participate fully and to furnish complete and accurate disruption information in a consistent, timely, and thorough manner.

DHS looks forward to reviewing the comments filed by the carriers on this issue and will carefully consider and evaluate any proposals concerning voluntary reporting schemes that may be advanced. In the spirit of partnership that has formed the foundation of NCS' effective relationship with industry, DHS stands ready to work with the Commission and the carrier community to explore any viable model that will ensure robust sharing of complete and accurate network disruption information on a non-mandatory basis in a manner that will support effective industry collaboration and appropriately safeguard the information.[22]

B. *Whether the Commission Adopts a Voluntary or Mandatory Framework, It Should Direct That Network Disruption Reports Be Filed In the First Instance with the NCC Telecom-ISAC.*

Regardless of whether the Commission adopts a voluntary or mandatory reporting framework, DHS strongly urges the Commission to consider having the network outage data be reported directly into NCS' National Coordinating Center for Telecommunications-Information Sharing and Analysis Center ("NCC Telecom-ISAC") via the secure electronic filing process outlined in the Notice,[23] rather than to the Commission.

Managed by IAIP/NCS, the National Coordinating Center ("NCC") is a joint industry-government operational body established in 1984 to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities under all

(..continued)
Government and one another, to address vulnerabilities and develop and refine best practices without mandating reporting in a way that publicly exposes potentially sensitive information.

[22] Such a framework, if combined with DHS' proposal that the information be reported into the NCC, see discussion *infra*, might enable DHS to afford Protected Critical Infrastructure Information (PCII) protection to the information, that would otherwise be unavailable. *See* 6 C.F.R. Part 29.

[23] *See id.* at 26 ¶ 50.

conditions, crises, or emergencies.[24] The NCC maintains a watch and analysis center (the NCC Operations Center) that has operated on a 24 x 7 basis since September 2001.[25]

The NCC Operations Center houses senior information assurance analysts who are closely integrated with the Federal government NCC operations staff and industry representatives from the NCC Telecom-ISAC member companies.[26] Full-time telecommunications industry representatives sit along side Government staff at the NCC Operations Center and serve as liaisons with their parent organizations for incident management. This integration fosters technical working relationships with external liaison partners, both in industry and Government. The technical expertise, collaboration efforts, and evolving analytical capability of the NCC have brought significant value to the information sharing process.

As a consequence of the cooperation and trust it has nurtured; its reputation as an "honest broker;" and its success as a central hub for sharing critical NS/EP telecommunications information among industry, and between Government and industry; the NCC was designated in January 2000 as the Telecommunications Information Sharing and Analysis Center.

---

[24] Since its creation, the NCC has coordinated the restoration and provisioning of NS/EP telecommunication services and facilities during natural disasters and armed conflicts, including the following events: Love Letter Worm Attack (5/00); Solar Sunrise Computer Attack (2/98); Illuminet SS7 Outage (2/98); Illuminet SS7 Outage (10/97); Red River Floods (4/97); Northwest Floods (1/97); Hurricane Fran (9/96); Oregon Floods (2/96); Hurricane Opal (10/95); Hurricane Marilyn (9/95); Louisiana Floods (4/95); Oklahoma City Bombing (5/95); Houston Floods (10/94); Georgia Floods (8/94); Miami Floods (4/94); Ice Storms (3/94); Northridge Earthquake (1/94); California Wildfires (11/93); Tulsa Flooding (4/93 - 5/93); Operation Provide Hope (12/92 - 11/93); Hurricane Iniki (9/92); Hurricane Andrew (8/92); Operation Desert Storm (1/91 - 3/91); Operation Desert Shield (4/90 - 1/91); Loma Prieta Earthquake (10/89); and Hurricane Hugo (9/89).

[25] During the recovery efforts following the terrorist attacks of September 11, 2001, the NCC provided national and regional level support for response and recovery efforts to government and industry organizations and personnel. The NCC prioritized the communications assets, and restoration efforts, thereby ensuring NS/EP telecommunications needs and national priorities were met. These coordination efforts, coupled with the cooperation among carriers and government that the NCC fosters, were also instrumental in achieving the restoration of service that enabled the financial markets to reopen less than a week following the attacks.

[26] At present, NCC Telecom-ISAC membership numbers six Federal government agencies and 32 private sector companies that provide telecommunications network services, equipment, or software to the communications and information technology sectors. These include Competitive Local Exchange Carriers (CLECs), Internet Service Providers (ISPs); and telecommunications professional organizations/associations. A complete list of the current members is appended hereto as Attachment A.

Under the Commission's existing rules, outage information must be reported to the Duty Officer in the FCC's Communications and Crisis Management Center.[27] The report is to be directed to NCS only in the event that the disruption constitutes a "mission-affecting outage" affecting "nuclear power plants, major military installations and key government facilities" and, even in that event, the report comes from the affected facility and NCS must contact the service provider to determine the anticipated duration of the outage, adding unnecessary delay to response efforts.[28]

While this framework may have appropriately accommodated the scope and nature of NCS' NS/EP responsibilities in 1992, when the rule was originally adopted, DHS respectfully submits that it no longer does so in the post September 11, 2001 environment. The structural realignment of NCS into DHS/IAIP, the directives set forth in HSPD-7, and the designation of the NCC as the Telecommunications ISAC all reflect the inescapable fact that the mission of NS/EP communications assurance is now, in many respects, co-extensive with that of telecommunications critical infrastructure protection for the civilian society and our economy – a point underscored by the significant degree to which other critical infrastructure sectors (*e.g.*, Banking and Financial Services, Emergency Services, Energy, and Transportation) depend upon reliable telecommunications for their own operations.

The Notice recognizes that one of the primary reasons for collecting outage data in the first place is to support response, recovery, and restoration of service in crisis situations. Directing the reporting to the NCC Telecom-ISAC will significantly augment the utility of outage data by most quickly and efficiently placing it where it can immediately be used for that

---

[27] *See generally* 47 C.F.R. § 63.100(b), (c), (d), and (e) (2003).

[28] *Id.* § 63.100(e), (e)(1). Section 63.100(a)(7) defines a "mission-affecting outage" as one that "is deemed critical to national security/emergency preparedness (NS/EP) operations of the affected facility by the National Communications System member agency operating the affected facility." *Id.* § 63.100(a)(7).

purpose in real time, while the event is unfolding. Directing the information in this way will also serve to enhance industry partnership, ensure effective reporting, enhance NS/EP planning and expand the collaborative efforts between DHS, the NCS and the Commission, thereby expediting and strengthening the analysis and collaboration that will lead to a more complete and more effective set of "best practices" for all service providers and private network operators.

DHS supports the Commission's proposal concerning electronic filing of disruption data for many of the reasons cited in the Notice. Such a submission mechanism would facilitate more rapid and efficient reporting; reduce the services providers' costs and the logistical effort associated with reporting; and make the outage data more readily available to the government and industry for analysis and collaboration.[29] Likewise, DHS believes that the electronic filing template proposed by the Commission[30] would effectively support ongoing best practice development and be of significant value to IAIP/NCS in planning for and carrying out its homeland and national security missions.

V. EXPANDED REPORTING MUST BE ACCOMPANIED BY APPROPRIATE MEASURES TO SAFEGUARD SENSITIVE DATA FROM UNAUTHORIZED DISCLOSURE

In several instances in the Notice, the Commission identifies what it believes to be the advantage of making outage reporting data generally accessible by the public: chiefly, the extent to which it facilitates the emergence of "best practices" by enabling service providers and manufacturers to learn from the collective experiences of the industry as a whole.[31] It observes

---

[29] *See Notice* at 26 ¶ 50. As discussed in the following section, however, DHS does have reservations about the apparent intention to use electronic filing to make reporting data more readily available to the public as a whole.

[30] *Id.* Appendix B.

[31] *See*, *e.g.*, *id.* at 6 ¶ 7 ("One benefit of this process has been that public access to outage reports has enable individual communications providers, as well as manufacturers, to learn directly from each other's outage experiences."); 8 ¶ 10 ("This process would likely not have been possible or so successful if service disruption reporting had not been mandatory and if those reports had not been available to communications providers, manufacturers, and the public."); 26 ¶ 50 ("Changes to outage report data should be more easily accessible by communications providers, the public, and the Commission.").

that such reports filed by wireline carriers have historically been publicly available, and invites comment concerning the application of this policy to the reports that will be filed by wireline, wireless, satellite, and cable service providers.[32]

DHS firmly believes that any expansion of the outage reporting rule adopted by the Commission must be accompanied by appropriate measures to safeguard reporting data to the maximum extent consistent with applicable information access laws. DHS understands that open access to government information and an informed citizenry are essential to the operation of our democratic system and to the missions of Federal agencies. However, as Congress has recognized, certain information that pertains to or affects our ability to protect the Homeland requires special safeguarding.[33] Outage reporting data (particularly that requested by the Commission in the proposed template) constitutes such information.

The data to be provided includes information concerning the direct and root cause(s) and duration of the disruption; the range and types of services affected; the scope and gravity of the impact across all platforms and geographic area; specific equipment failures; the specific network element(s) impacted; remedial measures and/or best practices applied; and an appraisal of the effectiveness of the best practices.[34] While this information is critical to identify and mitigate vulnerabilities in the system, it can equally be employed by hostile actors to identify vulnerabilities for the purpose of exploiting them.

Depending on the disruption in question, the errant disclosure to an adversary of this information concerning even a single event may present a grave risk to the infrastructure. The potential availability of all reports, across all of the platforms proposed in the Commission's Notice, could provide a potential adversary with a virtual road map targeting network stress

---

32 *Id.* at 27 ¶ 52.

33 *See* Act § 892(a)(1)(B), 6 U.S.C. § 482(a)(1)(B).

points and vulnerabilities and a field guide to defeating "best practices" and protective measures. The Commission's apparent proposal to make the outage reports available to the public electronically over the Internet increases this risk exponentially. Safeguarding this information – especially the location, root cause, provider and other sensitive information – should be a paramount consideration in the final rules adopted by the Commission.[35]

To this end, DHS again requests that the Commission consider adopting a framework whereby service providers submit outage reports to the NCC Telecom-ISAC, and that outage data be safeguarded from inappropriate use or disclosure. DHS is prepared to work with the Commission to assess what information is most sensitive and requires the greatest protection and to identify appropriate technical and procedural measures to safeguard this information. This need for safeguarding might be attenuated if public availability of the information was a prerequisite to realizing the benefits identified by the Commission, but it is not.

As previously discussed, the NCC Telecom-ISAC and NCS' Network Security Information Exchange ("NSIE") enable members of industry to share information with one another and with Government experts on both anomaly and systemically based vulnerabilities and provide an effective context supporting the development of best practices. These bodies did not exist when the original outage reporting requirement was implemented. Also, the ongoing efforts of the NRIC with public posting of industry best practices will continue and be made available to all industry providers and vendors. For these reasons, public availability of the

(..continued)

[34] *Notice* at 41-44, Appendix B.

[35] It is worthwhile to note that, if the vulnerability information in question were the Federal government's rather than the private sector's (that is, if it were "owned by, produced by or for, or [was] under the control of the United States Government"), it would be eligible for protection as classified national security information. *See* Executive Order No. 13292 of March 25, 2003, *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information*, 68 Fed. Reg. 15315, 15317 §§ 1.1(a), 1.4(g) (permitting classification of information that concerns "*vulnerabilities or capabilities of systems*, installations, *infrastructures*, projects, *plans, or protection services* relating to the national security, *which includes defense against transnational terrorism*." (emphasis added)).

detailed outage data is neither desirable nor is the need for it as compelling as it may have been in the past.

VI. THE COMMISSION SHOULD REEXAMINE THE SUITABILITY OF ITS 30-MINUTE/900,000 – USER MINUTES THRESHOLD FOR EACH OF THE INDUSTRY SEGMENTS TO BE COVERED BY THE RULES

The Commission also proposes to modify the standard to be used to determine when an outage report must be filed from 30,000 customers affected for 30 minutes or more to a disruption of 30 minutes or more that potentially affects 900,000 "user-minutes."[36] In addition, the Commission proposes to apply this "common metric" across all of the platforms that would be affected by the new rule – wireline, wireless, satellite, and cable.[37] In so doing, however, the Commission notes that "differences [among these platforms] may necessitate variations in developing the metric for these communications systems or even alternative approaches," and it invites comment on such possible approaches.[38]

As an initial matter, DHS agrees with the Commission's proposal to abandon affected "customers" as a reference point in favor of affected "users." This modification is appropriate to avoid the problem of non-reporting of potentially serious disruptions impacting significant numbers of end-users.

With respect to the proposed uniform application of the common metric across platforms, however, DHS believes that significant questions remain to be answered. Specifically, DHS questions whether the 30-minute/900,000-user minutes threshold is suitable or appropriate to apply to all segments and is concerned that it may result in some needed information not being reported. For example, with respect to satellite, DS3 minutes or cable segments, DHS wonders whether the proposed threshold may too high for the existing user base. Similarly, it is unclear

---

[36] *Notice* at 12-14 ¶¶ 19-23.

[37] *Id.* at 12-13 ¶ 21.

whether, in the wireless arena, the architectures of individual carriers call for a unique threshold for that platform.

Currently, the Notice appears to require outage reporting for the cellular segment based on network congestion.[39] However, network impacts caused by power outages or similar events are additional scenarios that warrant outage report consideration. In addition, the threshold for DS3 reporting seems set without consideration for compression, alternative coding and other rate reduction methods.

DHS is aware that a number of industry groups have been established to explore technical issues in relationship to specific segments regarding metrics and will defer further comment until these results are available. DHS agrees with the common metric approach but believes the thresholds, as applied to each segment, should be reviewed and specific technical guidance from industry group analysis be duly considered.

VII. CONCLUSION

DHS welcomes the opportunity to contribute to this important initiative. Through IAIP/NCS, DHS works daily with our partners in the private sector – the owners and operators of the nation's critical infrastructure – to secure America's telecommunications system against injury or attack. The service disruption information that wireline telecommunications providers have provided under the Commission's existing rules has contributed significantly to these efforts. The increasingly important role of non-wireline service providers in the telecommunications system makes it important to obtain the same disruption information from them.

Accordingly, DHS strongly supports the Commission's efforts in this proceeding to expand outage reporting in support of homeland security needs. However, the ultimate success

(..continued)

[38] *Id.*

[39] *Id.* at 19-20 ¶¶ 37-38.

of our critical infrastructure protection effort depends, in large part, not merely on having the necessary information, but on having it available when and where it is most needed. For this reason, DHS urges the Commission to consider having outage information filed directly with the NCC Telecom-ISAC and to explore appropriate measures consistent with law to safeguard this very sensitive information from disclosure to those who would use it for hostile purposes.

Respectfully submitted,

UNITED STATES DEPARTMENT OF HOMELAND SECURITY

By: /s/ Joe D. Whitley
Joe D. Whitley
General Counsel
United States Department of Homeland Security
700 D Street, S.W.
Washington, D.C. 20528
(202) 692-4232

/s/ Thomas J. Connelly
Thomas J. Connelly
Associate General Counsel for
Information Analysis and Infrastructure Protection
United States Department of Homeland Security
Nebraska Avenue Complex
Washington, D.C. 20528
(202) 692-4232

/s/ Eric T. Werner
Eric T. Werner
United States Department of Homeland Security
700 D Street, S.W.
Washington, D.C. 20528
(202) 401-0775

Date: June 2, 2004

ATTACHMENT A

NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS - INFORMATION SHARING AND ANALYSIS CENTER

Current Membership:

Federal Participants:

DHS
Department of Commerce
Department of Defense
Department of State
Federal Communications Commission
General Services Administration

Industry Members:

Americom
AT&T
AT&T Wireless
Avici
BellSouth
Boeing
Cable & Wireless
Cellular Telecommunications & Internet Association
Cincinnati Bell
Cingular Wireless
Cisco Systems
Computer Sciences Corporation
EDS
Intrado
Level 3 Communications
Lockheed Martin/Comsat Techologies
Lucent Technologies
MCI
McLeodUSA
Motorola
Nextel
Nortel Networks
Northrop Grumman
Qwest Communications
Raytheon
Science Applications International Corporation
SBC Communications
Sprint
Telecommunications Industry Association
United States Telecom Association
VeriSign
Verizon